

# NT4H console example user manual

## Version 1.1

# Table of contents

<b>Introduction</b>	<b>3</b>
<b>Application overview</b>	<b>3</b>
2.1 Get file setting (1)	4
2.2 Set file setting (2)	7
2.3. Get UID (3)	9
2.4. Set Random ID (4)	10
2.5 Change AES key (5)	10
2.6. Linear read (6)	11
2.7. Linear write (7)	12
2.8. Secure dynamic message read (8)	13
2.9. Secure dynamic message write (9)	14
2.10. Get SDM reading counter (a)	16
2.11. Store AES key into reader (b)	16
<b>Revision history</b>	<b>18</b>

# 1. Introduction

The NT4H is new serie of NXP NTAG® cards.

There are NTAG413 DNA, and NTAG424 DNA.

NTAG 424 DNA is fully compliant with the NFC Forum Type 4 Tag IC.

They are come with AES-128 cryptographic operation and a new Secure Unique NFC (SUN) Message.

## 2. Application overview

Link: <https://git.d-logic.net/nfc-rfid-reader-sdk/ufr-examples-c-nt4h>

On the picture is layout of application where used simple reader opening mode.

```
-----
      Please wait while opening uFR NFC reader.
-----
Select reader opening mode:
(1) - Simple Reader Open
(2) - Advanced Reader Open
-----
      uFR NFC reader successfully opened.
-----
+-----+
|              NT4H example              |
|              version 1.0                |
+-----+
                        For exit, hit escape.
-----
(1) - get file setting
(2) - set file setting
(3) - get UID (NTAG424 only)
(4) - set random ID (NTAG424 only)
(5) - change AES key
(6) - linear_read
(7) - linear write
(8) - secure dynamic message read
(9) - secure dynamic message write
(a) - get sdm reading counter
(b) - store AES key into reader
-----
Card type: DL_NTAG_424_DNA, sak = 0x20, uid[4] = 08:6B:09:11
-----
```

## 2.1 Get file setting (1)

The NTAG413 has two standard data files:

- File number 1 is Capability Container file (32 bytes)
- File number 2 is NDEF file (128 bytes)

The NTAG424 has three standard data files:

- File number 1 is Capability Container file (32 bytes)
- File number 2 is NDEF file (256 bytes)
- File number 3 is proprietary file (128 bytes)

Number of returned parameters is variable.

If current file is standard data file with AES secure messaging, then the following information is obtained:

- File type
- Communication mode
- File access rights
- File size

Example:

File number = 3 (NTAG424 proprietary file)

Communication mode is enciphered (0x03)

Secure dynamic messaging is disabled

Key number for read is 2,

key number for write is 3,

Key number for read/write is 3,

Key number for change file settings is 0,

File size is 128 bytes.

```
-----
                        Get file setting
-----

Enter file number (1 - 2 for NTAG413) (1 - 3 for NTAG424)
3

Get file setting successful
File type: Standard data file
Communication mode: enciphered
Secure dynamic messaging: disabled
File access rights (0x0E - free access, 0x0F - no access)
Read key: 0x02
Write key: 0x03
ReadWrite key: 0x03
Change key: 0x00
File size: 128
```



If current file is standard data file with secure dynamic messaging, then there are more informations.

Example:

File number is 2 (NDEF file).

Secure dynamic messaging is enabled.

Free access for reading and writing operations (key 0x0E)

File size is 256 bytes.

UID mirroring is enabled.

SDM reading counter is enabled.

SDM reading counter limit is disabled.

Encrypted part of file data uses.

Key number for SDM meta read is 2 (UID, SDM reading counter, PICC data, MAC)

Key number for encrypted part of file data is 2.

SDM reading counter can read without authentication.

PICC data offset (encrypted UID and SDM reading counter) is 49.

MAC input offset is 86.

Encrypted part of file data offset is 86.

Encrypted part of file data length is 32.

MAC offset is 124.



-----  
Get file setting  
-----

```
Enter file number (1 - 2 for NTAG413) (1 - 3 for NTAG424)
2

Get file setting successful
File type: Standard data file
Communication mode: plain
Secure dynamic messaging: enabled
File access rights (0x0E - free access, 0x0F - no access)
Read key: 0x0E
Write key: 0x0E
ReadWrite key: 0x0E
Change key: 0x00
File size: 256
Secure dynamic message options
UID mirroring: enabled
Read counter: enabled
Read counter limit: disabled
Encrypted part of file data: enabled
SDM access rights (0x0E free/plain, 0x0F no access/no data
SDM meta read: 0x02
SDM file key: 0x02
SDM reading counter read key: 0x0E
PICC data offset: 49
MAC input data offset: 86
Encrypted data offset: 86
Encrypted data length: 32
MAC offset: 124
```



## 2.2 Set file setting (2)

Due to the large number of parameters, there are two functions for setting file parameters.

Example:

Standard data file.

File number 3 (Proprietary file), current communication mode is enciphered, and change key number is 0.

New settings is: plain communication mode, read key 2, write key 3, read/write key 3, change key 0, authentication mode provided key

```
C:\WINDOWS\system32\cmd.exe

-----
                        Set file setting
-----

Select file type
(1) - Standard data file
(2) - Secure messaging data file

Enter file number (1 - 2 for NTAG413) (1 - 3 for NTAG424)
3

Enter change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424)
0

Select current communication mode
(1) - Plain mode
(2) - Macked mode
(3) - Enciphered mode
File access rights (14 - free access, 15 - no access)

Enter read key number (0 - 2 for NTAG413) (0 - 4 for NTAG424) or 14
2

Enter write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424) or 14 or 15
3

Enter read_write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424) or 0x14 or 0x15
3

Enter new change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424)
0

Select new communication mode
(1) - Plain mode
(2) - Macked mode
(3) - Enciphered mode
Select authentication mode
(1) - Provided key
(2) - Internal key
Enter change AES key (16 bytes hexadecimal)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Set file setting successful
```

Example 2:



Secure dynamic messaging file.

File number 2, communication mode plain, read key 14, write key 14, read/write key 14, change key 0, UID mirroring enabled, SDM reading counter enabled, SDM reading counter disabled, Encrypted part of data enabled, SDM meta read key 2, SDM file read 2, SDM reading counter key 2, Encrypted PICC data offset 49, MAC input data offset 86, Encrypted part of data offset 86, MAC offset 124.





### 2.3. Get UID (3)

NTAG424 DNA only.

Function returns 7 bytes long card UID. This is useful if the Random ID options activated.  
Valid authentication with any card key is required.

```
-----
                        Get UID
                        NTAG424 only
-----
Enter key number (0 - 4) 0
Select authentication mode
(1) - Provided key
(2) - Internal key
Enter AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Get UID successful
UID = 04:5B:A8:92:76:63:80
```

## 2.4. Set Random ID (4)

NTAG424 DNA only.

The card returns 4 bytes random ID instead 7 bytes unique ID.

Warning: this operation is irreversible.

Authentication with application master key (number 0) is required.

```
-----
                        Set random ID
                        NTAG424 only
-----
Select authentication mode
(1) - Provided key
(2) - Internal key
Enter AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Set random ID successful
```

## 2.5 Change AES key (5)

Authentication with application master key (number 0) is required.



If the key which will be changed is not master key, then old key value is required.

Example:

Key number 4.

Application master key value 0x00000000000000000000000000000000

Old key 4 value 0x00000000000000000000000000000000

New key 4 value 0x11111111111111111111111111111111

```
-----
                          Change AES key
-----
Enter key number (0 - 4)
4
  Select authentication mode
  (1) - Provided key
  (2) - Internal key
Enter master AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Enter new AES key (16 hexadecimal bytes)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
Enter old AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Change key successful
```

## 2.6. Linear read (6)

Function read data from file.

Required parameters are:

- File number
- Key number for read, or read/write access
- Communication mode
- Authentication mode (if read key is 14 then no authentication select)
- Start address (0 - max address)
- Length of data



```
-----  
                          Linear read  
-----  
Enter file number (NTAG413 1-2 NTAG424 1-3)  
3  
Enter key number (NTAG413 0-2 NTAG424 0-4)  
2  
Select communication mode  
(1) - Plain mode  
(2) - Macked mode  
(3) - Enciphered mode  
Enter linear address  
0  
Enter length  
128  
Select authentication mode  
(1) - Provided key  
(2) - Internal key  
(3) - No authentication  
Enter AES key  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
Liar read successful  
Hexadecimal:  
54:68:69:73:20:69:73:20:74:68:65:20:74:65:73:74:20:66:6F:72:20:6C:69:  
6E:65:61:72:20:64:61:74:61:20:77:72:69:74:65:20:69:6E:74:6F:20:66:69:  
6C:65:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  
ASCI:  
This is the test for linear data write into file
```

## 2.7. Linear write (7)

Function write data to file.

Required parameters are:

- File number
- Key number for write, or read/write access
- Communication mode
- Authentication mode (if read key is 14 then no authentication select)
- Start address (0 - max address)
- Data in ASCII or hexadecimal format





```
-----
                        Linear write
-----
Enter file number (NTAG413 1-2 NTAG424 1-3)
3
Enter key number (NTAG413 0-2 NTAG424 0-4)
3
  Select communication mode
  (1) - Plain mode
  (2) - Macked mode
  (3) - Enciphered mode
Enter linear address
0
Enter data
  (1) - ASCII
  (2) - HEX
Enter ASCII text
This is the test for linear data write into file
  Select authentication mode
  (1) - Provided key
  (2) - Internal key
  (3) - No authentication
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Liar write successful
```

## 2.8. Secure dynamic message read (8)

File must be in Secure dynamic message mode, and read access must be free (key no 14, no authentication required).



```
Secure dynamic message read
File number = 2, free read access, plain communication mode
-----
Raw hexadecimal data:
00:74:D1:01:70:55:00:68:74:74:70:3A:2F:2F:77:77:77:2E:74:65:73:74:2E:63:6F:6D:2F:6E:74:34:68:
3F:70:3D:38:44:43:31:44:37:35:34:42:37:42:38:39:32:30:38:36:37:32:35:43:33:38:37:41:43:35:42:
39:33:45:38:65:3D:30:32:46:42:41:32:38:35:42:45:35:33:31:45:43:30:36:42:36:44:46:31:43:34:34:
45:36:44:31:41:44:30:6D:3D:35:41:45:37:37:46:31:43:45:41:41:45:34:32:46:35:26:43:6D:61:63:3D:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
NDEF file context: http://www.test.com/nt4h?p=8DC1D754B7B892086725C387AC5B93E8e=02FBA285BE531
EC06B6DF1C44E6D1AD0m=5AE77F1CEAAE42F5&Cmac=

PICC encrypted data: 8DC1D754B7B892086725C387AC5B93E8
Enter meta data AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PICC data decrypted successful
UID = 04:5B:A8:92:76:63:80
Reading counter = 97

Encrypted part of file data: 02FBA285BE531EC06B6DF1C44E6D1AD0
Enter file data read AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Part of file data decrypted successful
Part of file data = test data

ASCII MAC data: 5AE77F1CEAAE42F5
ASCII MAC input data: 02FBA285BE531EC06B6DF1C44E6D1AD0m=
MAC is correct
```



15



## 2.10. Get SDM reading counter (a)

The Secure dynamic message reading counter exist only if in file settings enabled SDM.  
Depends of setting of SDM reading counter access, authentication required or not.

```
-----  
                        Get SDM reading counter  
-----  
Enter file number (NTAG413 2 NTAG424 2-3)  
2  
  Select authentication mode  
  (1) - Provided key  
  (2) - Internal key  
  (3) - No authentication  
Enter key number (NTAG413 0-2 NTAG424 0-4)  
2  
Enter AES key (16 hexadecimal bytes)  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
SDM reading counter = 84
```

## 2.11. Store AES key into reader (b)

Into reader may be stored 16 AES keys. Key number 0 - 15.

Example:

Store key 0x00000000000000000000000000000000 into reader in address 1.

```
-----  
                        Store AES key into reader  
-----  
  (1) - AES keys  
  (2) - Unlock reader  
  (3) - Lock reader  
  
Enter AES key  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
Enter key index (0 - 15)  
1  
  
Key written into reader
```



You can lock key into reader with 8 bytes password. By default keys are unlocked, and you can enter any password for locking.

Example:

Password is "12345678"

```
-----
                        Store AES key into reader
-----
(1) - AES keys
(2) - Unlock reader
(3) - Lock reader

Enter password of 8 bytes
(1) - ASCII
(2) - HEX
Enter ASCII text
12345678

Reader keys are locked
```

If keys are locked, you must unlocked them first with 8 bytes long password.

Example:

Password is "12345678"

```
-----
                        Store AES key into reader
-----
(1) - AES keys
(2) - Unlock reader
(3) - Lock reader

Enter password of 8 bytes
(1) - ASCII
(2) - HEX
Enter ASCII text
12345678

Reader keys are unlocked
```

## Revision history

Date	Version	Comment
2020-01-30	1.0	Base document